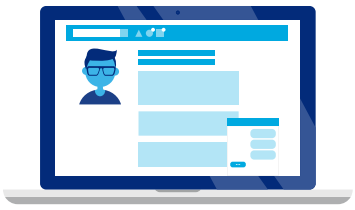
PROTECTING BUSINESS CUSTOMERS FROM ACCOUNT TAKEOVER FRAUD

Financial institutions play a critical role in not only securing and monitoring business accounts, but also in educating and training organizations (and their staff) on identifying suspicious communications and reducing organizational exposure. These measures can create a layered defense that makes account takeover fraud targeted at businesses harder to execute.

REDUCING EXPOSURE BEFORE CRIMINALS STRIKE

Account takeover fraud attacks often start with criminals gathering login credentials, employee details, and information about organizational processes and patterns. Reducing this exposure is a critical first step in prevention. Financial institutions can encourage their business customers to take these steps:

1. **Train employees to spot suspicious communications.** Criminals frequently use phishing emails, urgent phone calls or texts from an impersonated vendor to trick staff into revealing sensitive information. It can be difficult to recognize these attacks since criminals increasingly use generative artificial intelligence (AI) deepfakes, such as a video call in which an "executive" requests a large payment to a new vendor or account. Financial institutions can encourage their business customers to require their employees to verify any unusual requests through official processes and channels, especially requests involving payments or account access. A straightforward "pause and confirm" approach can stop attacks before they begin.



2. **Limit public exposure of sensitive roles within the organization.** Criminals often target individuals in finance or treasury positions because they control payment processes. Organizations should limit or avoid listing these roles publicly on social media or company websites and remind staff to keep professional details private where possible.

3. **Implement strong, unique passwords for business systems.** Reused or weak passwords are a common vulnerability abused by attackers for unauthorized entry into systems. Encourage business customers to implement password managers and enforce policies that prevent sharing credentials across platforms. By focusing on employee awareness, role confidentiality and password hygiene, financial institutions can help organizations close gaps that criminals exploit during the harvesting stage.

PROTECTING BUSINESS CUSTOMERS FROM ACCOUNT TAKEOVER FRAUD

SECURING ENTRY POINTS TO PREVENT ACCOUNT TAKEOVER FRAUD

Once credentials are harvested, attackers aim to gain access, and this is where strong controls make all the difference. Education and encouraging secure account access with a combination of biometrics and Multi-Factor Authentication (MFA) are some of the more effective ways to stop account takeover fraud before it escalates.

To start, financial institutions can strongly encourage business customers to adopt MFA for all authorized users of business accounts. This extra protection is especially important for employees who handle sensitive functions, such as payroll, finance, treasury or system administration. These roles often have access to accounts that can move money, update vendor payment information or change security settings, making them prime targets for criminals looking to take over business accounts. Adding MFA for these high-risk users helps prevent attackers from gaining control of systems that could cause significant financial or operational damage. Even when credentials are compromised, MFA significantly reduces the likelihood of unauthorized access. Financial institutions can encourage organizations to:

Educate staff about MFA fatigue. Criminals increasingly exploit employees who approve repeated MFA prompts without verifying the request's legitimacy. Companies should train users to have heightened scrutiny when approving unexpected requests and report suspicious activity immediately.

Regularly audit user access. Over time, employees accumulate permissions they may no longer need. This can create unnecessary risk. Organizations should regularly review and remove outdated or excessive access rights

Secure secondary accounts, such as email and vendor portals. These accounts often serve as backdoors for attackers to reset passwords or intercept sensitive communications. Applying MFA and strong password policies across all connected systems helps close these gaps.

Implement proactive monitoring. Daily reviews of account activity can provide critical safeguards. Account takeover fraud prevention is an ongoing effort. As fraud tactics evolve, so must defenses. By working together – financial institutions providing guidance and tools and businesses implementing best practices – organizations can build a multilayered defense that protects accounts, funds and customer trust.

PROTECTING BUSINESS CUSTOMERS FROM ACCOUNT TAKEOVER FRAUD

CONCLUSION: BUILDING A STRONG DEFENSE AGAINST ACCOUNT TAKEOVER FRAUD

Account takeover fraud prevention for businesses is not just about providing technology solutions, it is about working together with organizations to reduce their exposure, educate staff on phishing and suspicious requests, and implement robust authentication.

Companies can start by encouraging a "verify first" mindset. Employees should never approve unusual requests without confirming their legitimacy through trusted processes and channels. This simple habit can stop many attacks before they escalate. Combining this with strong authentication and regular audits of user access makes it harder for attackers to exploit stolen credentials. It ensures only authorized individuals have the permissions they need.

Equally important is employee awareness. Training staff to recognize phishing attempts, suspicious emails and MFA fatigue helps close the human vulnerabilities that criminals often exploit.

The account takeover fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.